UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/482,843	01/13/2000	Marcus Peinado	MSFT-0103/127334.6	7584

7590 08/12/2003

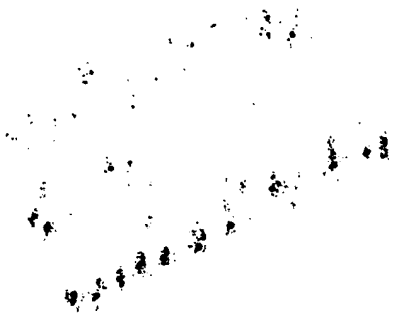
Steven H Meyer
Woodcock Washburn Kurtz Mackiewicz & Norris LLP
One Liberty Place
46th Floor
Philadelphia, PA 19103

EXAMINER
NGUYEN, CUONG H

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 08/12/2003

Please find below and/or attached an Office communication concerning this application or proceeding.



Office Action Summary

Application No.	Applicant(s)
09/482,843	Marcus Peinado et al.
Examiner	**Art Unit**
Cuong H. Nguyen	3625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *May 21, 2003* .

2a) ☒ This action is **FINAL.** 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *106-135* is/are pending in the application.

4a) Of the above, claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *106-135* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☒ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)

16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____

18) ☐ Interview Summary (PTO-413) Paper No(s). _____

19) ☐ Notice of Informal Patent Application (PTO-152)

20) ☐ Other:

DETAILED ACTION

1. This Office Action is the answer to the response received on 5/21/2003 (the Reconsideration, paper # 6).

2. Claims 106-135 are pending in this application.

Response

3. 35 USC 112, 2nd para. : On claims 106, and claim 121, the examiner submits that "lacking an antecedent basis for "the package being separate and apart from the license", the examiner means about structural relations between them is lacking. Applicants' arguments have been fully considered but they are not persuasive with 35 U.S.C.§101, and previous cited references for 35 U.S.C.§103(a) rejections. On page 3, para.3, the applicants argue that "the examiner is incorrect in characterizing the content of the package as a computer program per se", the examiner submits that claim 121 clearly indicates that claim 106 's package contains programs in a computer-readable medium; that claim 106 contains digital components is merely an exemplary of the invention; based on the Guidelines ,claims 106-120 recite computer programs per se. The examiner reviewed thoroughly the cited prior art again and he recognizes that those cited references are obvious with what the applicants claimed.

3A. Re. To claims **106**, and **121**: In e-commerce, placing 2 things that are attached together or making them separate in one package are obvious (i.e., in these claims, claiming a license for a digital content and that digital content placing separately is not inventive concerning that if Stefik package attached these 2 together); applicants argue that "Stefik package would not include

license acquisition information for acquiring a license" because "the license is already attached to the Stefik package and thus need not be acquire", the examiner submits that an analogous answer as "putting together a digital content & a license in one single package or putting them separately are not inventive" because claim 106 is about a single package, and claim 121 is about a single computer-readable medium that may have different file/directory for contents or license, although they are separate "file" but they are in the same computer-readable media, i.e., a floppy disk (for the argument on page 7, para. 1, received on 5/21/2003). The examiner did rejects this feature under obviousness (35 USC 103 (a)) with Stefik and Krisna 's inventions.

- (for the argument on page 7, para. 2, received on 5/21/2003) about a package ID, it is obvious with Stefik's patent that in order to distinguish one from another; it is obvious with ordinary skill in the art to "label" them differently for retrieval in a computer as Stefik's system (Fig.12 – ref. 1207 is just an example of "how" the Stefik's computer would "select" a descriptor storage or a content storage; it is obvious that Stefik's system having components' identifications). The examiner did rejects this feature under obviousness (35 USC 103 (a)) with Stefik's patent.

- (for the argument on page 9, para. 2, received on 5/21/2003) about "a certificate to include a public key of a content provider", this is old and well-known for an apparatus claim for putting 2 things together in a package (claim 116/131) (e.g. see **Stefik,** 42:48-52, 43:29-35) this indicates that "a digital certificate and a public key" are sent to a customer together (e.g., in a single

package) in order to use a public key from said certificate). One with ordinary skill in the art would send these 2 components together although only a public key would be utilized by the receiver. The examiner did rejects this feature under obviousness (35 USC 103 (a)) with Stefik, Krisna 's patent, and further in view of the Official Notice.

For the argument on page 9, para.5 (received on 5/21/2003), the examiner submits that claimed features are obvious from the capabilities of Stefik, and Krisna 's computer system; this is a general observation and detail rationale/references were supplied in the Office Action.

The examiner provides evidences that prove the obviousness of claimed limitations for taking Official Notices; these evidences suggest that claimed features are not inventive:

3B. Re. To claims **107**, and **122**:

- a license information is encrypted (e.g., see **Mullor** et al., claim 15 of US Pat. 6,411,941).

3C. Re. To claims **108**, and **123**:

- a license provider location is a network address. (e.g., see Coley et al. US Pat. 5,790,664, - in Detailed Description Text portion (para.8):

"Once the connection is confirmed (step 206), the client module 103 forms a license validity inquiry request message (step 208). The request message may contain information such as the application name, the application version number, a date/time stamp, the name of a license server 110 (if several license servers are maintained by the software provider), and a hardware identifier, such as the IP address of the computer 100 ».

3D. Re. To claims **109**, and **124**:

- a license provider location is an Internet address (e.g., see Clark, US Pat. 6343280, in Detailed Description Text portion (para. 38):

"FIG. 14 depicts a block diagrammatic overview of the operation of the Trap Software 6 determining, connecting to, and executing the Modified Software 7 in cooperation with the License Server 4 (selected from a set of available License Server's 4) having the fastest network response time at the time of the Trap Software's 6 request for service from the License Server 4. In order to locate the fastest network route to a License Server 4, software object 266 (contained within the Trap Software 10) communicates 264 a "ping" message to each License Server 4 known to software object 266 in order to determine which License Server 4 has the fastest network response time. A "ping" measures the amount of time it takes a small packet of bytes to travel to and from a given network address, in this instance the address of each of the known License Servers 4. By measuring the average ping time to each License Server 4, an estimate can be formed as to which License Server 4 will provide the fastest service for the Trap Software's 6 request. Software object 266 communicates 274 the ping information (network address of the License Server 4 providing the quickest response time) to software object 267 which then acts to make a network connection from the Software User 2 to the best (smallest average ping time) License Server 4. Software object 267 communicates 268 to software object 25 that the connection to the License Server 4 has been established, and software object 25 begins executing the Modified Software 7. The Modified Software 7 continues to execute as described previously until a Trap/Breakpoint is encountered or the execution terminates. While the Modified Software 7 executes, software object 25 periodically communicates 276 to software object 269 the request to search for the License Server 4 having the quickest network response time. Software object 269 communicates 265 an identical ping query to each of the known License Servers 4. The results of the network ping query is communicated 277 by software object 269 to software object 270 which checks to see if a faster route to a License Server 4 was found. If software object 270 determines that a faster route than the route to the currently connected License Server 4 was found, then the network address of the License Server 4 having the faster ping query response time is communicated

278 by software object 270 to software object 271 which terminates the connection with the License Server 4 having the slower ping query response time and makes a connection to the License Server 4 having the faster ping query response time. Software object 271 then communicates 272 a control signal to software object 269 where the process of making a ping query of all known License Servers 4 is repeated periodically while the Modified Software 7 continues to execute. If software object 270 determines that a faster route (a network connection having a lower ping query response time) to a License Server 4 was not found, then software object 270 does not communicate 278 a new License Server 4 network address to software object 271 whereby the Software User 2 stays connected to the previously selected License Server 4 and software object 270 communicates 273 a reset signal to software object 269. In this manner, the Trap Software 6 always maintains a connection".

3E. Re. To claims **110**, and **125**:

- a package having a public key, and a private key, and encrypted public key (e.g., see Epstein US Pat. 6023510, the summary and claim 1).

3F. Re. To claims **111**, and **126**:

- a provider's public key is encrypted (e.g., see Epstein US Pat. 6023510, claim 1).

3G. Re. To claims **112-113**, and **127**:

- an **encrypted** public key is signed by a private key (note: "and wherein alteration of the encrypted content provider public key prevents validation of the package" is a "functional description phrase", it would not be considered having weight for such an apparatus claim) (e.g. see **Sudia** US Pat. 6,009,177 "Brief Summary Text (13):

Another system of digital signature, called DSA for Digital Signature Algorithm, may also be used for sender verification. The DSA Algorithm was disclosed in U.S. patent application Ser. No. 07/738,431, which is hereby incorporated by reference in its entirety. The DSA Algorithm has properties that are

similar to those of the RSA signature algorithm in that the sender passes the message through a hashing algorithm to produce a message digest and then encrypts or signs the message digest using his private key; the recipient verifies the encrypted digest using the-sender's public key. However, unlike the RSA signature algorithm that returns the original message digest when the recipient decrypts the signature block, the DSA verification algorithm results only in a positive confirmation of the validity of the signature; communications encrypted using an intended recipient's public key cannot later be recovered by decryption with the recipient's corresponding private key. For this reason, the DSA algorithm may be used quite capably for digital signatures, but not for key transport or for direct message encryption".

3H. Re. To claims **114**, and **129**:

- an ID for a decryption key (e.g., see Sims III, US Pat. 6,550,011 "Detailed Description Text (28):

The most preferred embodiment compliant information storage device also includes secure areas for storing one or more secure data sets. Such data sets may include an identification of the data set, such as a simple enumeration, content decryption keys, content use information, and public keys and their corresponding signatures. These data sets are preferably associated with particular protected works, providing association to the content of content keys and information regarding any restrictions on use of the content (content use information).").

3I. Re. To claims **115**, and **130**:

- a certificate (in said package) about said provider (see Sims III, US Pat. 6,550,011 "Detailed Description Text (48):

"Transmission of the certificates is particularly useful in situations where the destination device is a less known device, such as provided by a relatively small company or is a relatively new device, and does not appear on the source device's list of acceptable devices. If the certificate is provided by a certificate authority that the content provider trusts, the certificate should be acceptable proof of the device's compliance.").

3J. Re. To claims **116**, and **131**:

- said certificate having a public key provider (see Wiser et al., US Pat. 6,385,596 "Detailed Description Text (29):

Referring to FIG. 4 there is shown an embodiment of a passport. Each passport includes a consumer certificate 402, a consumer private key 412, encrypted personal information 414, and a registration key 420. The consumer certificate 402 is used to authenticate the purchaser of a media data file 200, and to encrypt a purchased media data file 200. The certificate 402 is preferably in the ISO X.509 format, and issued by a trusted certificate authority, which in the preferred embodiment is the media licensing center 110. Each consumer certificate 402 in the ISO X.509 format includes a consumer public key 404, set of validity dates 406 defining the period during which the certificate is valid, a serial number 408, and a digital signature 410 of certificate authority."; or see Sims III, US Pat. 6,550,011 "Detailed Description Text (63):

At step 307 the computer provides to the storage device the public key for the acceptable use device and/or a certificate from an acceptable certificate authority. The storage device will preferably verify the public key and/or certificate and encrypt future communication with that public key or the public key associated with the certificate.").

3K. Re. To claims **117, 120, 135**, and **132**:

- a certificate is signed with a private key (note: "and wherein alteration of the encrypted content provider public key prevents validation of the package" is a "functional description phrase", it would not be considered having weight for such an apparatus claim) (e.g., see Gruse et al. US Pat. 6,389,538, "Detailed Description Text (359):

Electronic Digital Content Store(s) Certificate--A certificate provided to the Electronic Digital Content Store(s) 103 by the Clearinghouse(s) 105 and signed by the Clearinghouse(s) 105 using its private key. This certificate is used by the End-User Player Application 195 to verify that the Electronic Digital Content Store(s) 103 is a valid distributor of Content 113. The End-User Player Application 195 and

Clearinghouse(s) 105 can verify that the Electronic Digital Content Store(s) 103 is an authorized distributor by decrypting the certificate's signature with the Clearinghouse's 105 Public Key 621. The End-User Player Application 195 keeps a local copy of the Clearinghouse's 105 Public Key 621 that it receives as part of its initialization during installation.").

3L. Re. To claims **118**, and **133**:

- a package with a first certificate and a second certificate (note: claim 118 would be interpreted like the above because this claim is directed to a physical package; it would be old and well-known that a certificate represents an authorization), (e.g., see Sudia et al., US Pat. 5,995,625, claim 41).

3M. Re. To claims **119**, and **134**:

- a first certificate and a second certificate having their public keys (note: claim 119 would be interpreted like the above because this claim is directed to a physical package and what possess by a content provider (or an intermediary source) is not part of the claimed package) (e.g., see Geer Jr. et al., US Pat. 6,212,634 "Detailed Description Text (31):

In the event that there are multiple conversations between multiple subsets of the computers monitored by the arbiter, the arbiter can create a set of conversation certificates corresponding to each of the respective conversations. For example, if initially there is a conversation between two of the computers and then three additional computers join in, the arbiter can initially create a conversation certificate for the two computers, which it distributes to the two computers only, and then when the arbiter is notified that three additional computers will be joining, the arbiter creates a new conversation certificate and distributes it to all five computers. The arbiter records, as the final entry in the message log for the first conversation, a link to the message log for the second conversation, encrypted with the private key for the first conversation, which the arbiter then destroys. The arbiter records, as the first entry in the message log for the second conversation, a link to the message log for the first conversation, encrypted with the private

key for the second conversation. The two parties to the first conversation can read the first message log by decrypting the messages using the public key contained in the first certificate, and all five parties can read the second message log by decrypting the messages using the public key contained in the second certificate.").

4. Since the examiner is examining an utility patent, the claims must be directed to systems, methods or articles of manufacture that have a clear utility. See MPEP 706.03(a) for example. Over the years, numerous court decisions have analyzed the content of various claimed language for meaningful, useful differences in structure or acts performed between the claims and the prior art. Some of these decision have found that certain language adds little, if anything, to the claimed structure or acts and thus do not serve as a limitation on the claims to distinguish over the prior art. For example, language directed to an intended use for a system of in a claim that does not result much in a structural or functional difference with respect to prior art were held not to serve as a limitation on the claim. See in re **Schreiber**, 44 USPQ2d 1429 (CAFC 1997).

Thus, a limitation on a claim can broadly be thought of then as its ability to make a meaningful contribution to the definition of the invention in a claim. In other words, language that is not functionally interrelated with the useful acts, structure, or properties of the claimed invention will not serve as a limitation. See in re **Gulack**, 217 USPQ 401 (CAFC 1983), ex parte **Carver**, 227 USPQ 465 (BdPatApp&Int 1985) and in re **Lowry**, 32 USPQ2d 1031 (CAFC 1994)

where language provided certain limitations because of specific relationships required by the claims.

Claim Rejections - 35 USC §101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requires of this title.

6. Claims **106-120** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. These claims are merely directed to a software package (standing alone), and that package contains computer program per se (see "Examination Procedures for Computer-Related Inventions – 2/27/1996, box 6" a USPTO guideline); this package (by itself) do not produce a useful, tangible, concrete result (without being act on by something else, that "something else" must be claimed to make that "computer program per se" become meaningful) according to "State Street" case.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112 (claims 106, & 121):

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7.A. Re. To claim **106**: It lacks an antecedent basis for "the package being separate and apart from the license" in line 3, page 2 (of claim 106) submitted

on 1/13/2000; this claim is about a package; however, based on above limitation, the license stands on its own (not in the claimed package).

This claim is also unclear about a meaning of term(s): "a content/package ID" (on page 3, line 3). For clarification, the examiner submits to replace above phrase with – a content or a package ID --.

This phrase is unclear "identifying one of the digital content and the package". It would be contradict to "a content/package ID".

7.B. Re. To claims **121**: This claim is unclear for:

A similar deficiency of claim 106 is repeated; that is claim 121 is about a medium with a data structure only. Then, from where "a license" comes from; should it be contained in that claimed medium or not in that medium; in the second case (if not in said medium) the examiner submits that "a digital license" can not be weighted as part of a limitation in claim. The above problem of "a content/package ID" should also be corrected to avoid indefinite problems.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C.§ 103(a) which forms the basis for all obviousness rejections set forth in this Office Action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

9. Claims **106-135** are rejected under 35 U.S.C.§ 103(a) as being unpatentable over **Stefik** (US Pat. 5,715,403), in view of **Krishnan**, (US Pat. 6,073,124).

A. Re. To claims **106, 121**: **Stefik** discloses a structure including:

a field containing encrypted digital content "The requester records the work contents, data, and usage rights. It then creates a one-time key and encrypts the contents file. It saves the key information in a restoration file.

Detailed Description Text (341):

'In some cases, it is convenient to be able to archive the large, encrypted contents file to secure offline storage, such as a magneto-optical storage system or magnetic tape" to be rendered in accordance with a corresponding digital license, the data structure being separate and apart from the license, the encrypted digital content being decrypt-able according to a decryption key (KD) "Each repository has given the other a key to be used in decrypting further communications during the session. Since that key is itself transmitted in the public key of the receiving repository only it will be able to decrypt the key which is used to decrypt subsequent messages." obtained from the license "Since licenses are themselves digital works, the same mechanisms give the creators control over distributors by charging for licenses and putting time limits on their validity".

Detailed Description Text (444):

"A creator purchases a digital distribution license that he will hand out to his distributors. He puts access requirements (such as a personal license) on the Copy and Transfer rights on the distribution license so that only he can copy or transfer it".

Detailed Description Text (484):

"The creator creates a digital work, an upgrade ticket, and a distribution license.";

- a field containing a content/package ID identifying one of the digital content and the package (see **Stefik**, Fig.12 – ref. 1207;

Stefik does not expressly disclose a field containing license acquisition information including a location of a license provider.

However, **Krishnan** et al. clearly disclose above point, see **Krishnan** et al., "in Table 1 the CommerceServer field indicates the location of the licensing and purchasing broker (e.g., the network address of licensing and purchasing broker 307 in FIG. 3) to be used to license and purchase the merchandise.".

- (see **Stefik** "FIG. 4b is an example of a computer system as a rendering system. A computer system may constitute a "multi-function" device since it may execute digital works (e.g. software programs) and display digital works (e.g. a digitized photograph). Logically, each rendering device can be viewed as having it's own repository, although only one physical repository is needed. Referring to FIG. 4b, a computer system 410 has contained therein a display/execution repository 411. The display/execution repository 411 is coupled to display device, 412 and execution device 413. The dashed box surrounding the computer system 410 represents a security boundary within which communications are assumed to be secure. The display/execution

repository 411 is further coupled to a credit server 414 to report any fees to be billed for access to a digital work and a repository 415 for accessing digital works stored therein."; and "The hardware embodiment of a repository will be enclosed in a secure housing which if compromised, may cause the repository to be disabled. The basic components of the hardware embodiment of a repository are described with reference to FIG. 12. Referring to FIG. 12, a repository is comprised of a processing means 1200, storage system 1207, clock 1205 and external interface 1206. The processing means 1200 is comprised of a processor element 1201 and processor memory 1202. The processing means 1201 provides controller, repository transaction and usage rights transaction functions for the repository. Various functions in the operation of the repository such as decryption and/or decompression of digital works and transaction messages are also performed by the processing means 1200. The processor element 1201 may be a microprocessor or other suitable computing component. The processor memory 1202 would typically be further comprised of Read Only Memories (ROM) and Random Access Memories (RAM). Such memories would contain the software instructions utilized by the processor element 1201 in performing the functions of the repository.

And "...The user interface itself need not be part of the repository. As a repository may be embedded in some other device, the user interface may merely be a part of the device in which the repository is embedded. For example, the repository could be embedded in a "card" that is inserted into an available slot in a computer system. The user interface may be combination of a display,

keyboard, cursor control device and software executing on the computer system.").

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of **Stefik**, with **Krishnan**'s idea in a software program, because artisan in this specific field would appreciate extra information of "a location of a license provider" for extra and complete information relating to a digital content.

B. Re. To claim **122**: The data structure of claim 121 wherein the license acquisition information is in an unencrypted form. The examiner submits that it is obvious to one with skill in the art that "license acquisition information" is not necessary for encryption since this information can be obtain in many web sites.

C. Re. To claims **123/124**: The data structure of claim 121 wherein the license provider location is a network/Internet address. The examiner submits that it is obvious to one with skill in the art that "license provider location is a network/Internet address" since network/Internet addresses have been very popular for accessing in communications at the time of filing this pending application.

D. Re. To claim **125**: The data structure of claim 121 wherein the data structure is provided by a content provider having a public key and a private key, the data structure further including a field containing the content provider public key (see Stefik, "At this point, assuming that the transaction has not terminated, the repositories exchange messages containing session keys to be used in all communications during the session and synchronize their clocks. FIG. 17

illustrates the session information exchange and clock synchronization steps (again from the perspective of repository-1.) Referring to FIG. 17, repository-1 creates a session key pair, step 1701. A first key is kept private and is used by repository-1 to encrypt messages. The second key is a public key used by repository-2 to decrypt messages. The second key is encrypted using the public key of repository-2, step 1702 and is sent to repository-2, step 1703. Upon receipt, repository-2 decrypts the second key, step 1704. The second key is used to decrypt messages in subsequent communications. When each repository has completed this step, they are both convinced that the other repository is bona fide and that they are communicating with the original. Each repository has given the other a key to be used in decrypting further communications during the session. Since that key is itself transmitted in the public key of the receiving repository only it will be able to decrypt the key which is used to decrypt subsequent messages.").

E. Re. To claim **126**: The data structure of claim 125 wherein the content provider public key is encrypted according to the decryption key (see **Stefik**, "Because the communication line is assumed to be unsecured, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well-known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public

keys are those that are distributed to others. Private keys are maintained in confidence.").

F. Re. To claim **127**: The data structure of claim 126 wherein the encrypted content provider public key is signed by the content provider private key, and wherein alteration of the encrypted content provider public key prevents validation of the data structure (see **Stefik**, "Because the communication line is assumed to be unsecured, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.")..

G. Re. To claim **128**: The data structure of claim 125 wherein the content provider public key is signed by the content provider private key, wherein alteration of the content provider public key prevents validation of the data structure (see **Stefik**, "Because the communication line is assumed to be unsecured, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking

keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.").

H. Re. To claim **129**: The data structure of claim 121 further comprising a field containing a key ID identifying the decryption key (see **Stefik**, "Each repository has given the other a key to be used in decrypting further communications during the session. Since that key is itself transmitted in the public key of the receiving repository only it will be able to decrypt the key which is used to decrypt subsequent messages.").

I. Re. To claim **130**: The data structure of claim 121 wherein the data structure is provided by a content provider authorized by a root source to provide the data structure, the data structure further comprising a fourth data field containing a certificate from the root source indicating that the content provider has authority from the root source to provide the data structure.

J. Re. To claim 131: The data structure of claim 130 wherein the content provider has a public key and a private key, and wherein the certificate includes the public key of the content provider.

K. Re. To claim 132: The data structure of claim 131 wherein the root source has a public key and a private key, wherein the certificate is signed with the private key of the root source, and wherein the public key of the root source must be obtained to decrypt the encrypted signature.

L. Re. To claim 133: The data structure of claim 121 wherein the data structure is provided by a content provider authorized by an intermediary source

to provide the data structure, the intermediary source in turn being authorized by a root source to authorize the content provider, the data structure further comprising a fourth data field containing a first certificate from the root source indicating that the intermediary source has authority from the root source to authorize the content provider, and a fifth data field containing a second certificate from the intermediary source indicating that the content provider has authority from the intermediary source to provide the data structure.

M. Re. To claim 134: The data structure of claim 133 wherein the content provider has a public key and a private key, wherein the intermediary source has a public key and a private key, wherein the first certificate includes the public key of the intermediary source, and wherein the second certificate includes the public key of the content provider.

N. Re. To claim 135: The data structure of claim 134 wherein the root source has a public key and a private key, wherein the first certificate is signed with the private key of the root source, wherein the second certificate is signed with the private key of the intermediary source, wherein the public key of the root source must be obtained to decrypt the encrypted signature of the first certificate, and wherein the public key of the intermediary source is obtained from the first certificate to decrypt the encrypted signature of the second certificate.

O. Re. To claim **106**: This claim obviously contains similar features as in claim **121**, although "a digital package" is claimed (since said package is merely

placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

P. Re. To claim **107**: This claim obviously contains similar features as in claim **122**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

Q. Re. To claim **108**: This claim obviously contains similar features as in claim **123**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

R. Re. To claim **109**: This claim obviously contains similar features as in claim **124**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

S. Re. To claim **110**: This claim obviously contains similar features as in claim **125**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

T. Re. To claim **111**: This claim obviously contains similar features as in claim **126**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

U. Re. To claim **112**: This claim obviously contains similar features as in claim **127**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

V. Re. To claim **113**: This claim obviously contains similar features as in claim **128**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

X. Re. To claim **114**: This claim obviously contains similar features as in claim **129**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

Y. Re. To claim **115**: This claim obviously contains similar features as in claim **130**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

W. Re. To claim **116**: This claim obviously contains similar features as in claim **131**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

AA. Re. To claim **117**: This claim obviously contains similar features as in claim **132**, although "a digital package" is claimed (since said package is merely

placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

AB. Re. To claim **118**: This claim obviously contains similar features as in claim **133**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

AC. Re. To claim **119**: This claim obviously contains similar features as in claim **134**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

AD. Re. To claim **120**: This claim obviously contains similar features as in claim **135**, although "a digital package" is claimed (since said package is merely placed on a computer-readable medium). Therefore, similar rationales and references set forth are applied for rejection under 35 U.S.C.§ 103(a).

The examiner submits that all claimed limitations are already capabilities of cited computer system, because these claimed limitations are very broad that they are recognized to be included as software components of a digital rights management system in cited prior art; cited prior art limitations are not necessary spelled-out exactly claimed languages, because cited prior art are also directed to a similar system for managing digital rights. **Krishnan**, **Stefik**, or submitted IDS references are not limited to the described embodiments in their inventions since they are exemplary examples. It is reasonable that various modifications of the described method and system of the cited prior art would be apparent to those skilled in the art without departing from

the scope and spirit of the invention. Although their invention has been described in connection with specific preferred embodiments, it should be understood that their invention as claimed should not be limited to such specific embodiments.

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Stefik, and **Krishnan**, with suggestions readily available in the art submitted in the IDS, because artisan in this specific field would appreciate these disclosed information for improvement of communication and security in a digital right management system.

Conclusion

10. Claims **106-135** are not patentable. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicants are reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. These references are considered pertinent to applicants' disclosure.

- Krishnan, (US Pat.6073124 – 6/06/2000), Method and system for securely incorporating electronic information into an online purchasing application

- Stefik, (US Pat. 5,715,403), discloses about a system for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar.

- Stefik et al., (US Pat. 5,629,980), discloses about a system for controlling the distribution and use of digital works.

- Van Wie et al., (US Pat. 5,943,422), discloses about a steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels.

- Ginter et al., (US Pat. 5,982,891), discloses about a system and a method for secure transaction management and electronic rights protection.

- **Rabne** et al., (US Pat. 6,006,332) teach about a rights management system for digital media.

- **Shear** et al., (US Pat. 6,112,181) teach about systems and methods for matching, selecting, narrow casting, and classifying based on rights management .

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cuong H. Nguyen whose telephone number is 703-305-4553 The examiner can normally be reached on Mon.-Fri. from 7:00 AM to 3:15 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ms. Wynn Coggins, can be reached on (703)308-1344.

Any response to this action should be mailed to:

Amendments